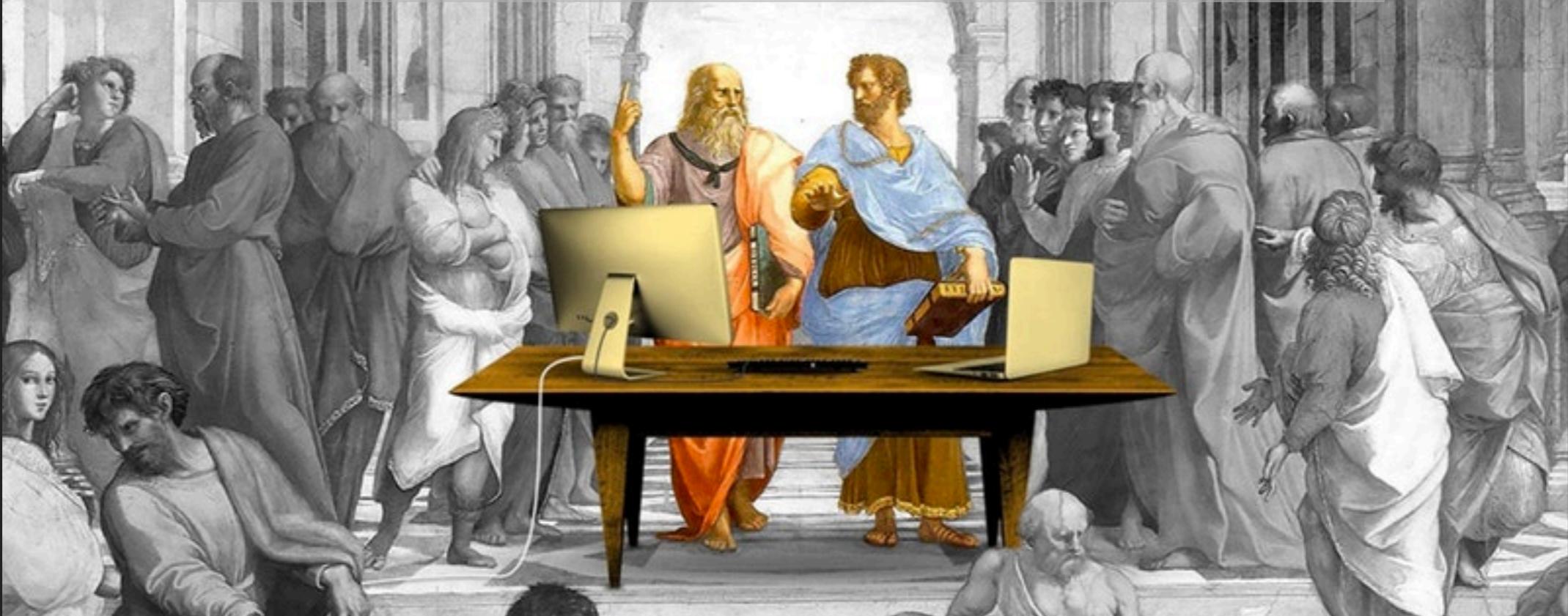


SECURE DELAWARE 2017



BLOCKCHAIN SECURITY

INIGO THOMAS, Ph.D., CISSP

BLOCK OF DATA + CHAINED TOGETHER

TRANSACTIONS	BLOCK INFO	# TXS	HEIGHT	BROADCASTED
40/f5a58242d71512ba3fcc2648dfe544d..	4e4c14d3f7..	597	366568	9 minutes ago
c7ca902bd54cfab642845c89ae617d13f0ab..	2ff8115475..	2040	366567	14 minutes ago
8dbf2791f8252f4c5ccfe7834494f74cadb..	34b1998f05..	2065	366566	30 minutes ago
4d42db50915dff2a48f978a7a1457f8e1fa..	260affrd50..	594	366565	an hour ago
10bb6a730a10bb31583b8011e5528006f693..	4a354a0cdd..	671	366564	2 hours ago



OUTLINE

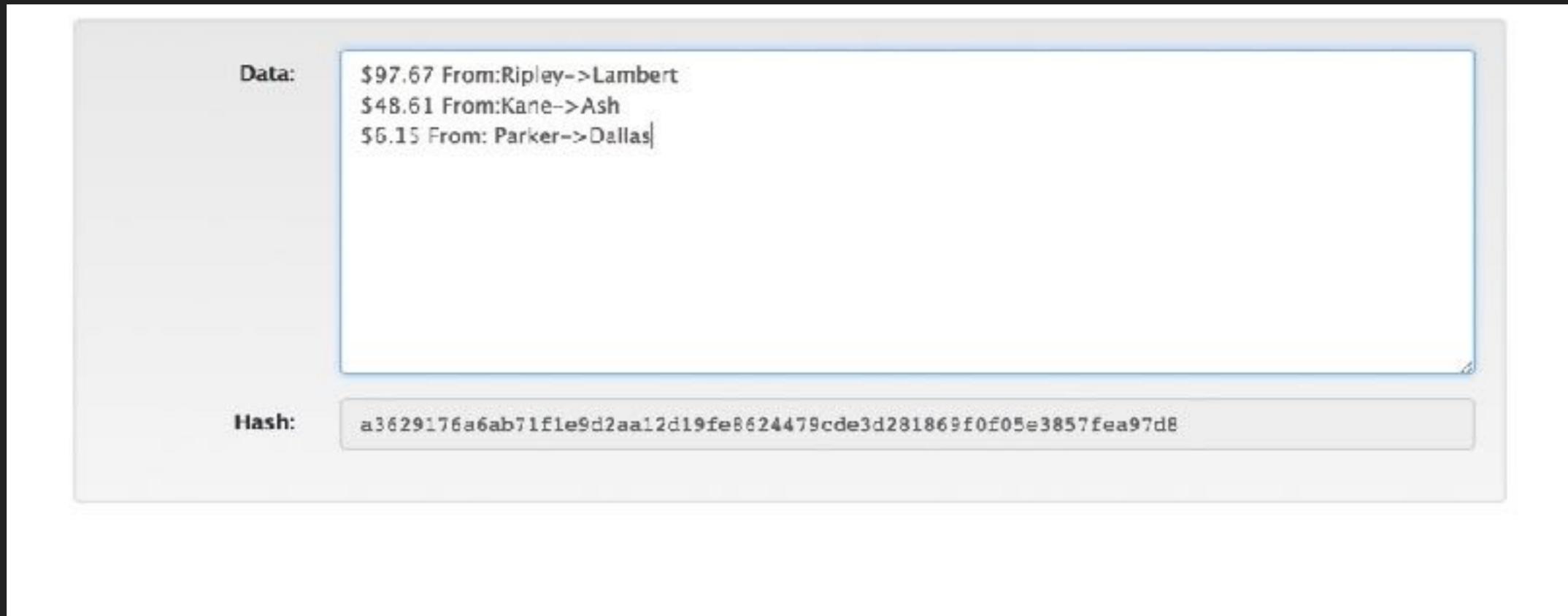
- ▶ BLOCKS
- ▶ USE CASES
- ▶ WALLETS
- ▶ EXCHANGES
- ▶ MINING
- ▶ THE \$55M HEIST
- ▶ YOUR OWN - AZURE



Go to: tlk.io/sd2017



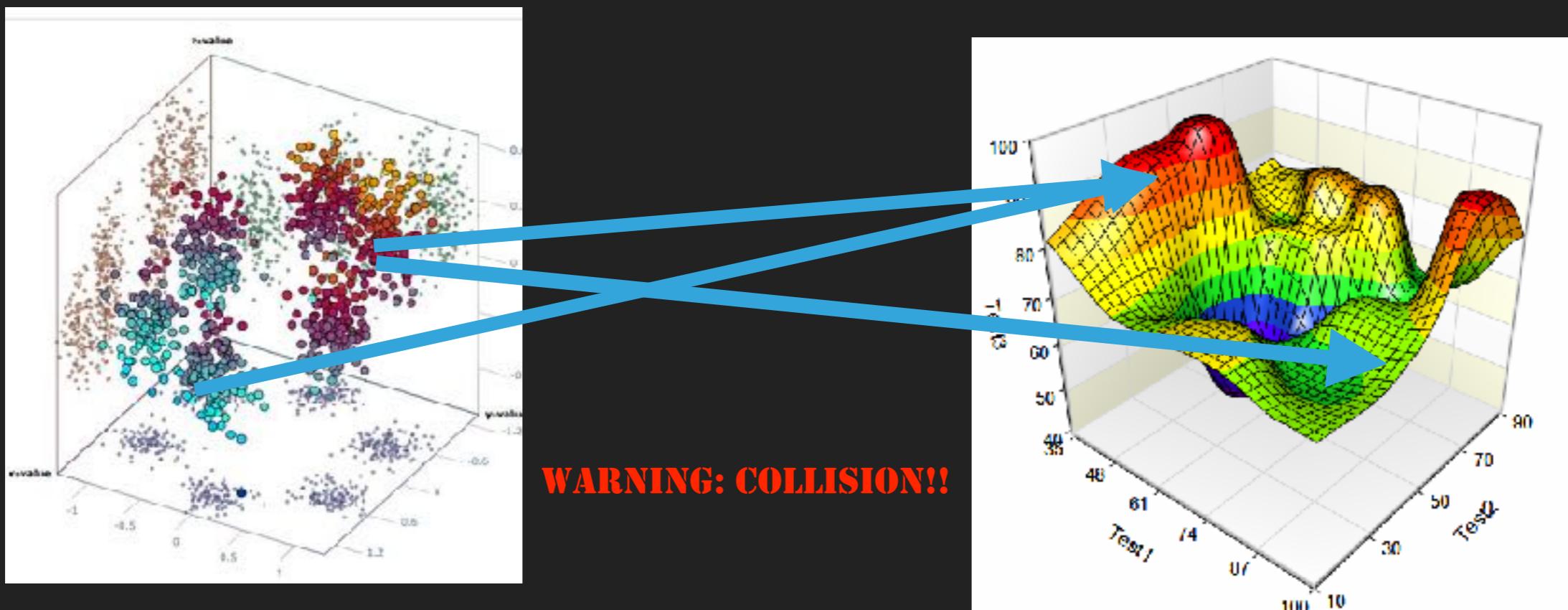
HASH



Go to: anders.com/blockchain/hash.html

HASHING SECURITY

- ▶ Based on Diffusion (Shannon, 1945)
- ▶ Changing one input bit -> changes many output bits
- ▶ $\text{bit}(i) \text{ flips} \Rightarrow 0.5 \text{ chance } b(j) \text{ flips}$

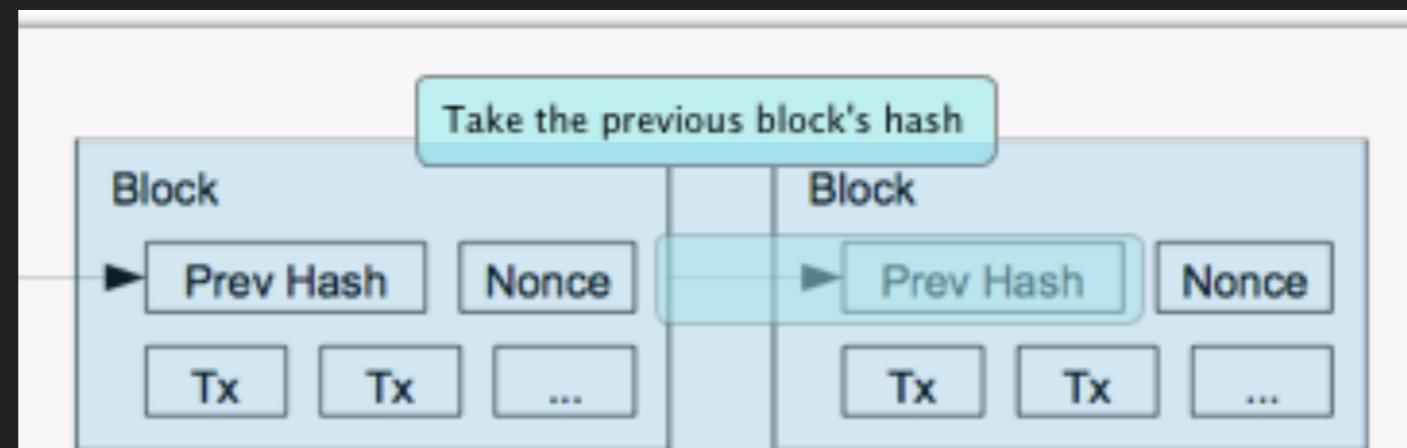


BLOCKS

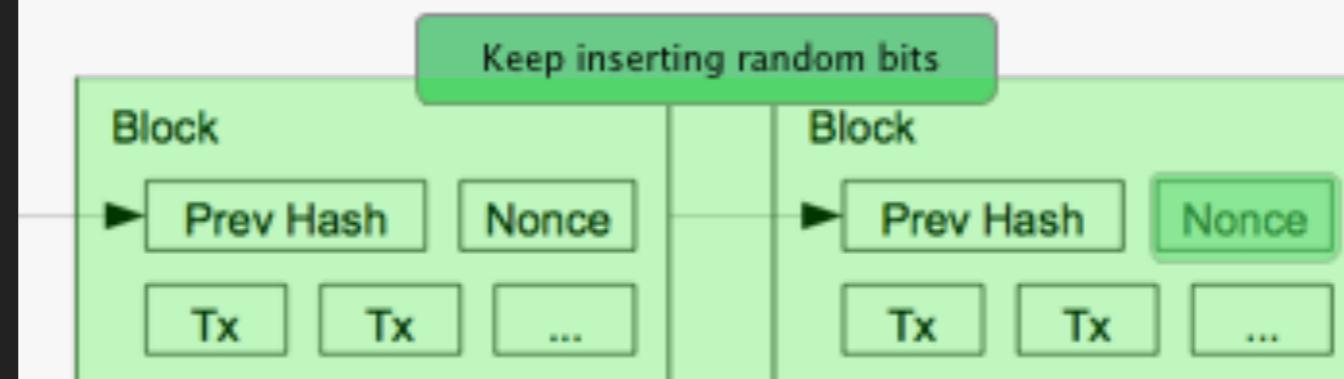
Block:	#	2
Nonce:	39207	
Tx:	\$ 97.67	From: Ripley -> Lambert
	\$ 48.61	From: Kane -> Ash
	\$ 6.15	From: Parker -> Dallas
	\$ 10.44	From: Hicks -> Newt
	\$ 88.32	From: Bishop -> Burke
	\$ 45.00	From: Hudson -> Gorman
	\$ 92.00	From: Vasquez -> Apone
Prev:	00000c52990ee86de55ec4b9b32beefd745d71675dc0edd	
Hash:	000078be183417844c14a9251ca246fb15df1074019873f	

BLOCK CHAIN

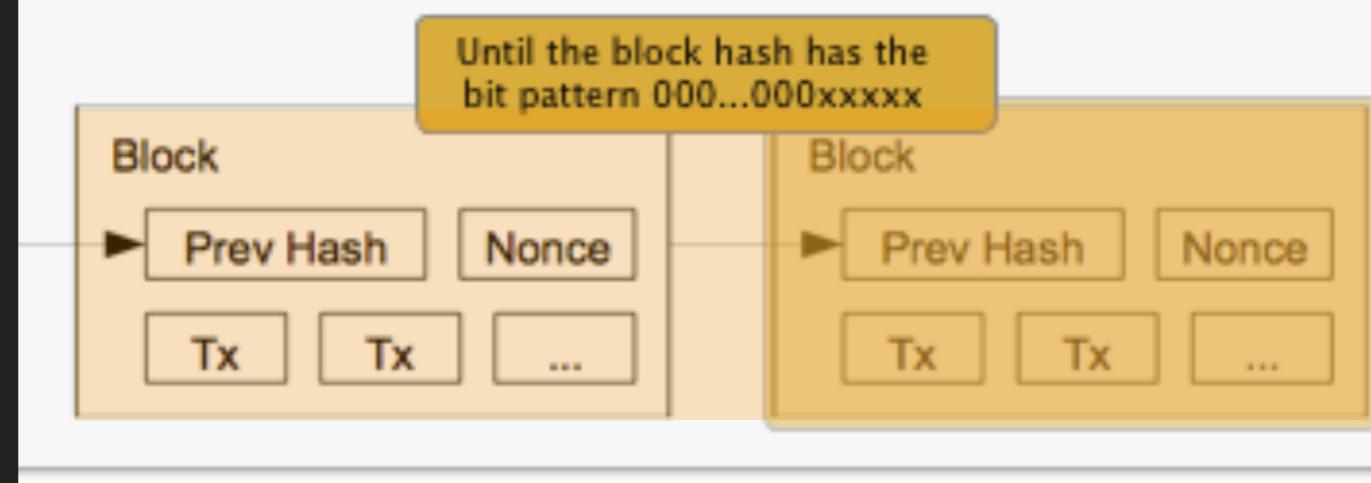
1



2



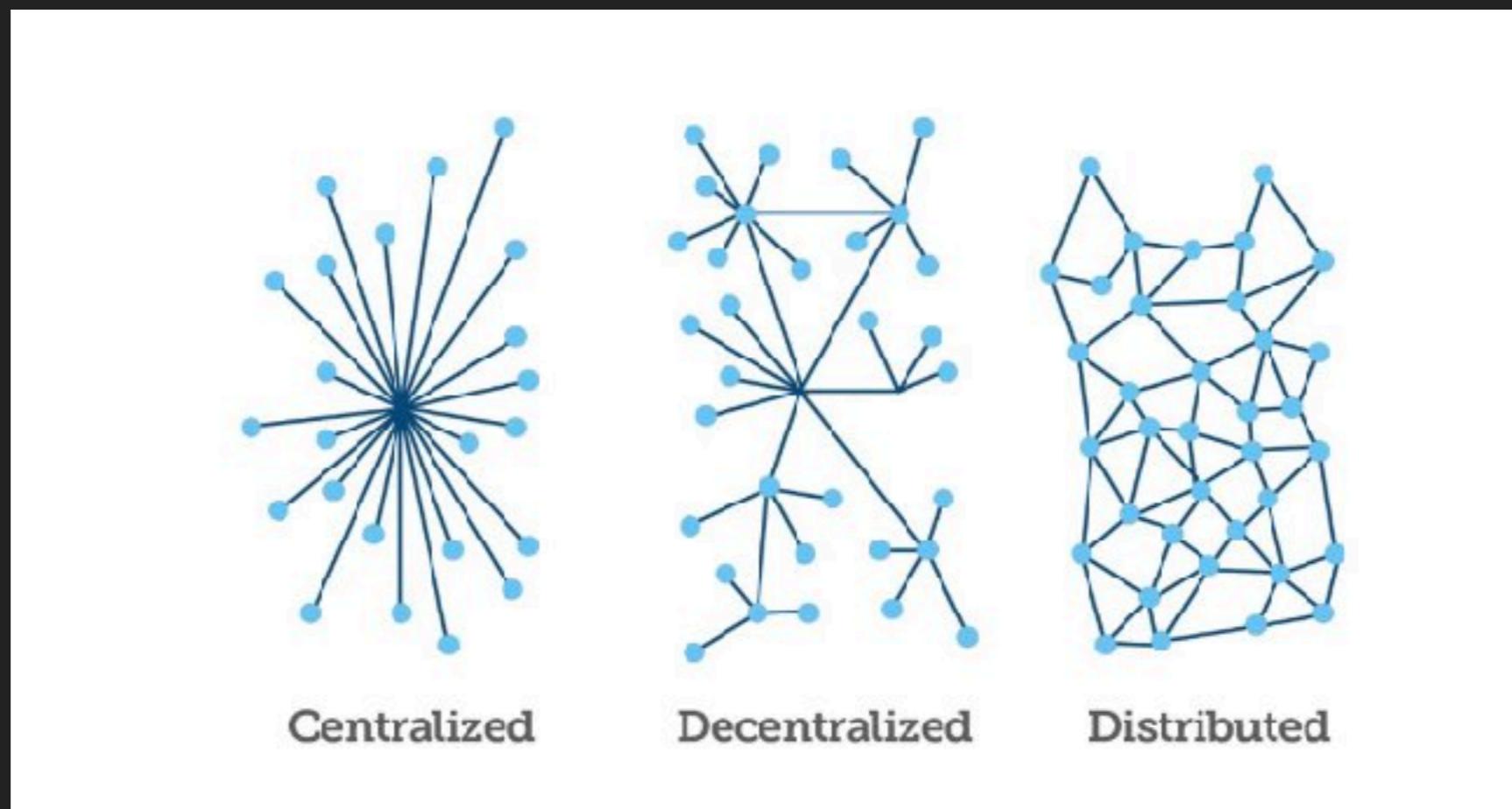
3



DEMO

Go to: anders.com/blockchain/blockchain.html

OTHERS VS. BLOCKCHAIN



USE CASES

- ▶ Cryptocurrency
- ▶ Micro Insurance
- ▶ Crowd Funding
- ▶ Corporate Shares
- ▶ Supply Chain



CRYPTOCURRENCIES

Total Market Cap: \$148,901,359,024

#	Name	Symbol	Market Cap	Price
1	Bitcoin	BTC	\$73,306,658,625	\$4416.25
2	Ethereum	ETH	\$28,259,177,344	\$297.72
3	Ripple	XRP	\$7,725,824,013	\$0.201488
4	Bitcoin Cash	BCH	\$7,107,797,056	\$426.92
5	Litecoin	LTC	\$2,870,790,805	\$53.97

100	Vertcoin	VTC	\$40,932,544	\$1.02
101	Elastic			
1144	FedoraShare	FEDS	?	\$0.000008
102	FairCoin			
1145	Lepaoquan	HLB	?	\$0.002153
103	iExec RLC			
1146	Quartz	QRZ	?	\$0.000037
104	ZCoin			
105	Dentacoin	DCN	\$38,344,278	\$0.000127

BITCOIN (JANUARY 2009 – PRESENT)

DECEMBER 15, 2010

“Why Bitcoin can’t be a currency” – The Underground Economist | \$0.23

JUNE 20, 2011

“So, That’s the End of Bitcoin Then” – Forbes | \$15.15

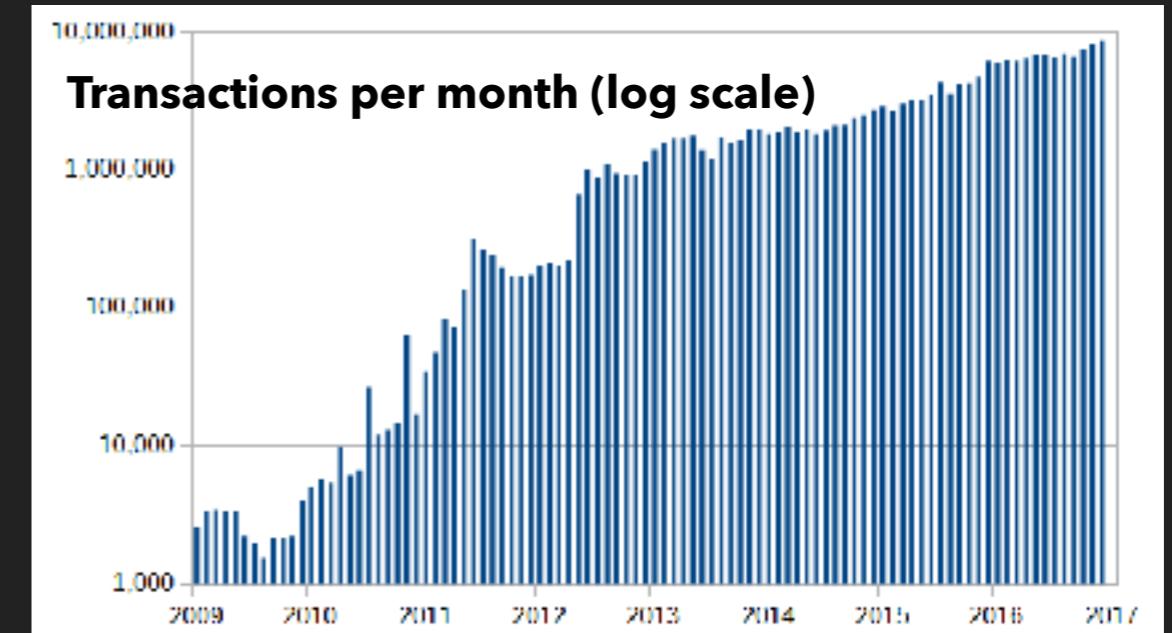
FEBRUARY 25, 2014

“Mt. Gox Meltdown Spells Doom for Bitcoin” – Bloomberg
\$532.71

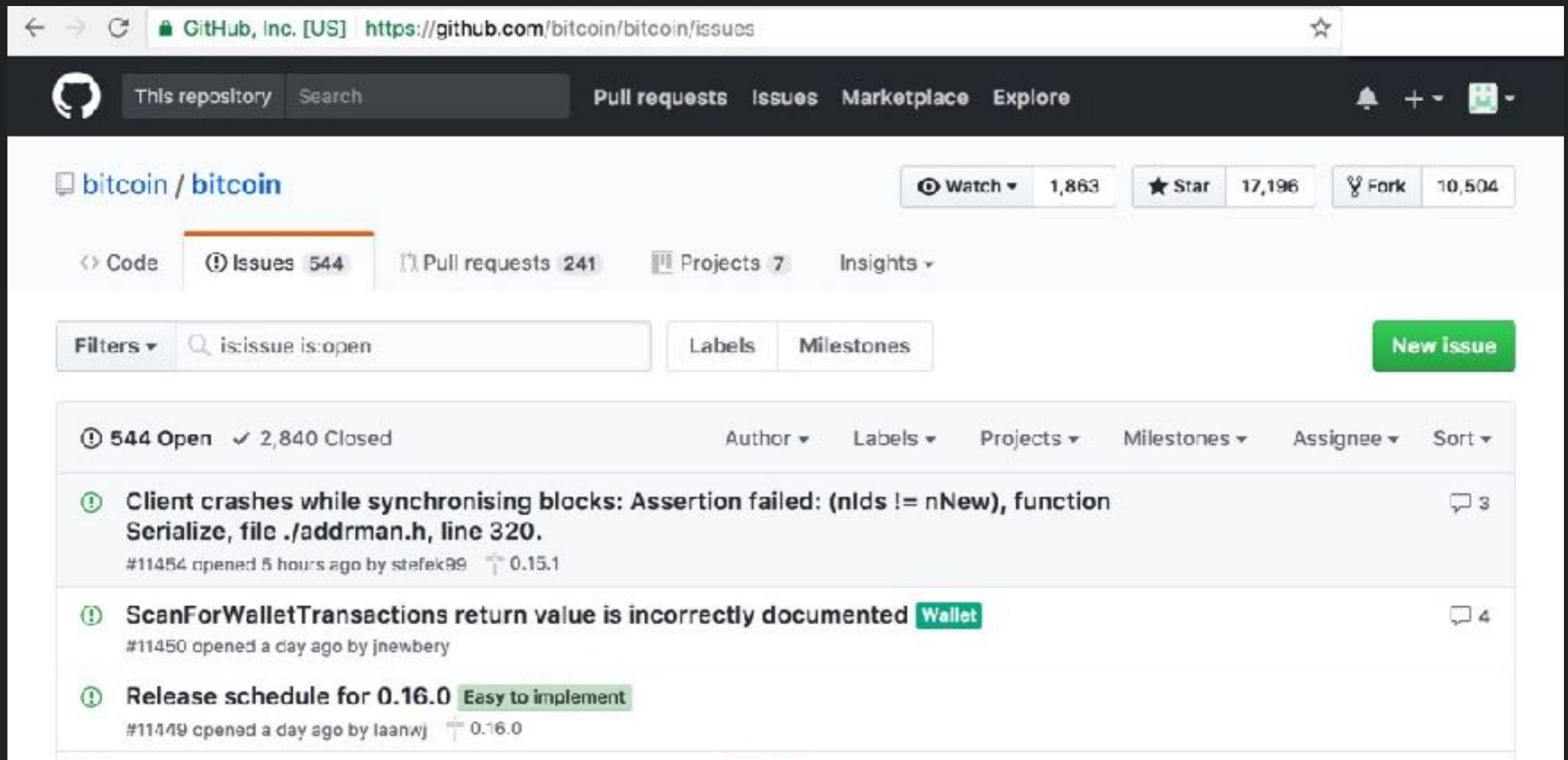
SEPTEMBER 12, 2017

“JPMorgan CEO Jamie Dimon says bitcoin is a ‘fraud’ that will eventually blow up” – CNBC | \$4,367.12

Bitcoin has died 171 times



BITCOIN SECURITY



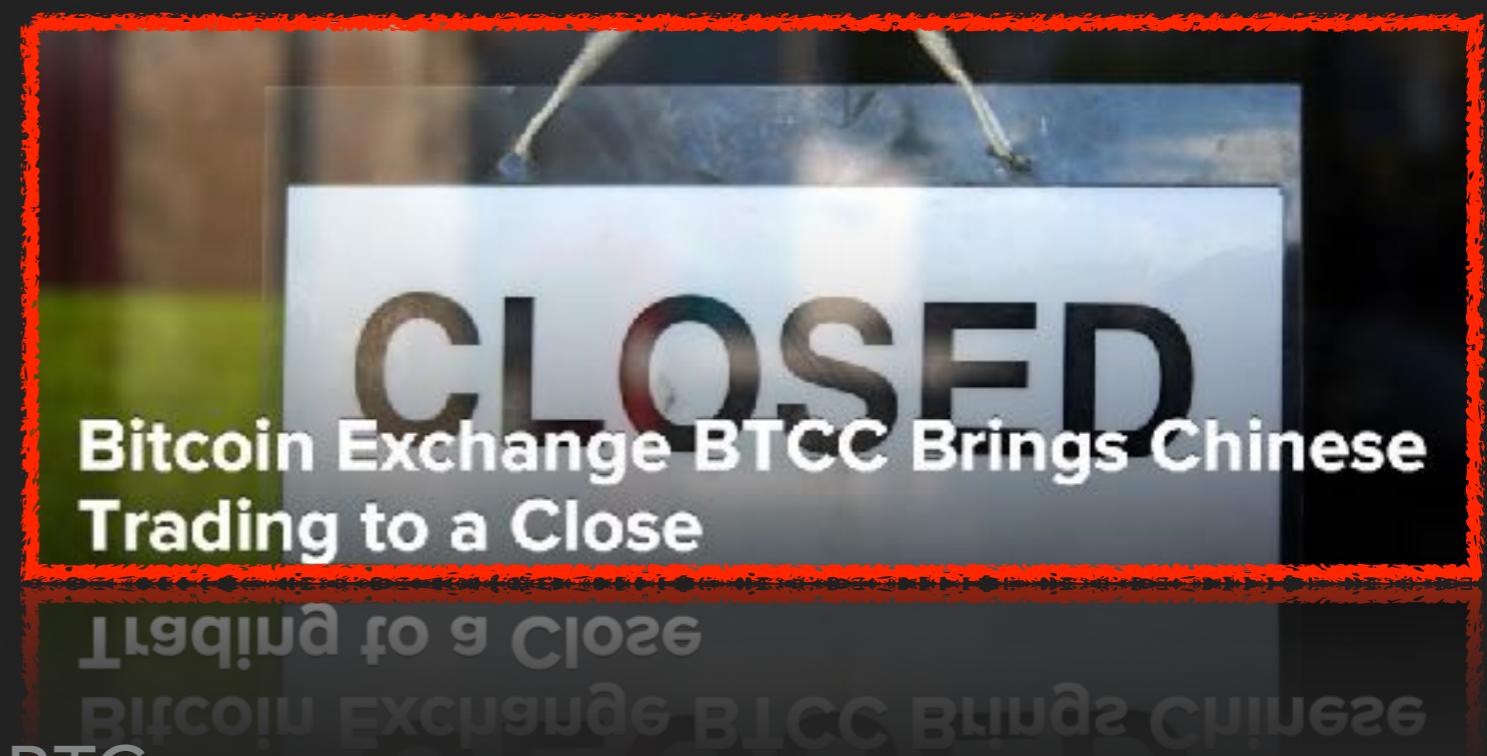
The screenshot shows the GitHub interface for the repository `bitcoin / bitcoin`. The top navigation bar includes links for Pull requests, Issues, Marketplace, and Explore. The Issues tab is selected, showing 544 open issues and 2,840 closed issues. A search bar filters issues by status: `is:issue is:open`. Below the filters, there are buttons for Labels and Milestones, and a prominent green "New issue" button. The main list of issues includes:

- #11454 Client crashes while synchronising blocks: Assertion failed: (nIds != nNew), function Serialize, file ./addrman.h, line 320.** (3 comments) - Opened 5 hours ago by stefek99, assigned to 0.15.1
- #11450 ScanForWalletTransactions return value is incorrectly documented** (4 comments) - Opened a day ago by jnewbery, assigned to Wallet
- #11449 Release schedule for 0.16.0** (Easy to implement) (1 comment) - Opened a day ago by laanwj, assigned to 0.16.0

- ▶ Inflation: 8/15/2010, 184 billion BTC, detected < 1.5 hours, patched < 4 hours

EXCHANGES

- ▶ To trade to fiat or other cryptocurrencies
- ▶ Bitstamp - Slovenia
- ▶ Bitfinex - Hong Kong
- ▶ Coinbase - San Francisco
- ▶ Coincheck, Coinfloor, itBit, , BTC-e, Kraken, BTCCChina, etc.

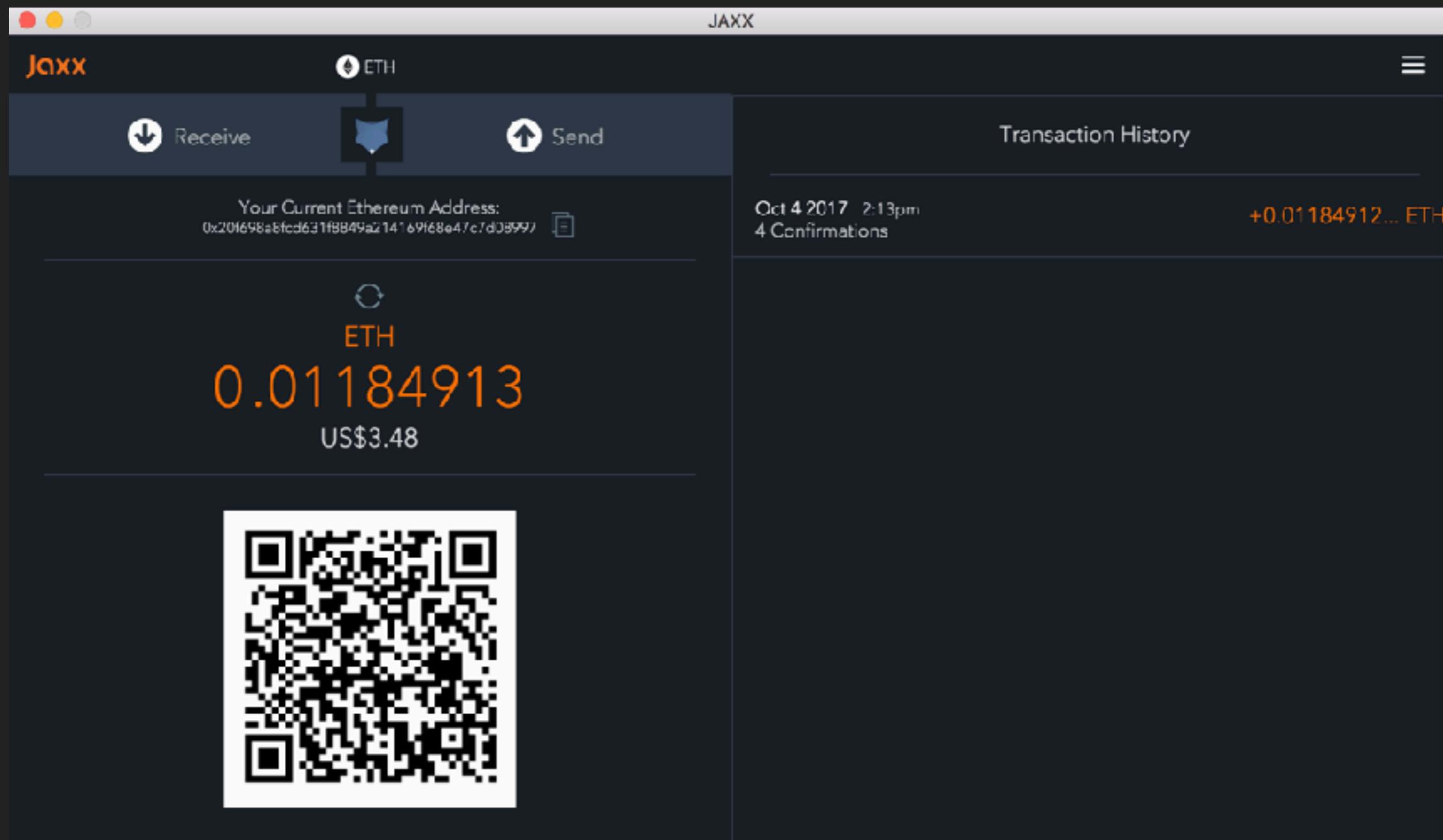


EXCHANGES SECURITY

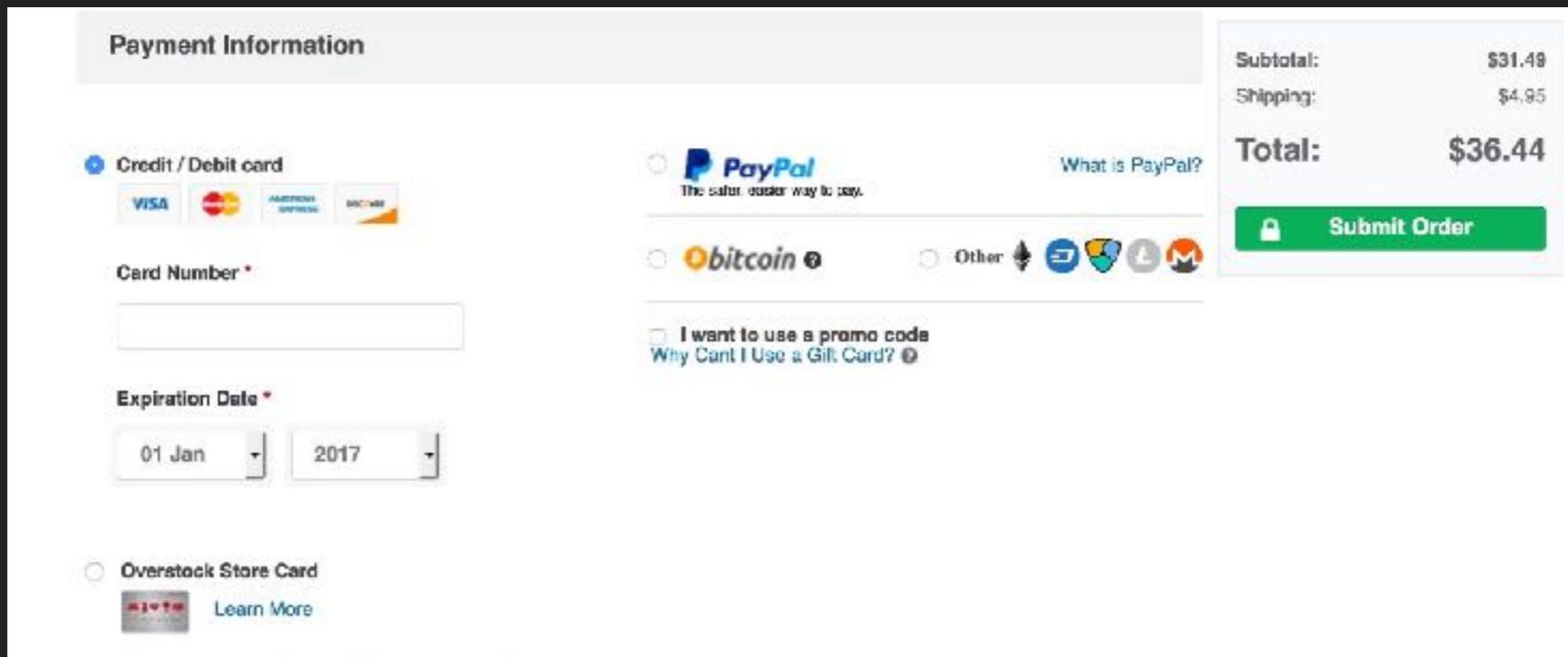
- ▶ Mt. Gox February 2014, \$450 M
- ▶ Bitfinex August, 2016 - \$72 M stolen
- ▶ Bitthumb , S. Korea's largest, June 2017, >\$1M
- ▶ Bitstamp April 2015, \$5M
- ▶ [inputs.io](#) Oct, 2014, \$1.2M
- ▶ DDOS of Major Exchanges
- ▶ Linode, Bitcoinica, Bitfloor, BIPS, etc.



DIGITAL WALLETS - JAXX.IO



PAYMENTS WITH BITCOIN



- ▶ Microsoft, DISH, Intuit, Japan, S. Korea
- ▶ Goldman Sachs - currency trading?!

XAPO.COM

xapo

WE'VE BUILT A FORTRESS

Secure bitcoin storage is what we do best. We've developed a new standard in bitcoin security that protects your assets by using man, machine and even a mountain to keep your money safe.

DEEP UNDERGROUND VAULTS IN THREE CONTINENTS

SERVERS NOT CONNECTED TO THE INTERNET

GUARDED 24/7.

DIGITAL WALLET SECURITY



...IS YOUR RESPONSIBILITY!

ETHEREUM

The screenshot shows the Ethereum wallet interface. At the top, there are navigation icons for Wallets, Send, and Contracts, along with network information (TEST-NET, 0 peers, 14,250 blocks, 3s since last block) and a balance of 15,573,027.80 USD. Below this, the "ACCOUNTS" tab is selected, displaying the main account details: Main Account (ETHERBASE) with a balance of 15,573,027.80 USD and address 0x5cc507A5ABb3ca63a4e37c26D61a0e87c0B0dFB4. There is also a button to "ADD ACCOUNT". At the bottom, the "WALLET CONTRACTS" tab is visible.

BALANCE
15,573,027.80 USD

TEST-NET 0 peers | 14,250 blocks since last block

WALLETS SEND CONTRACTS

Accounts Overview

ACCOUNTS

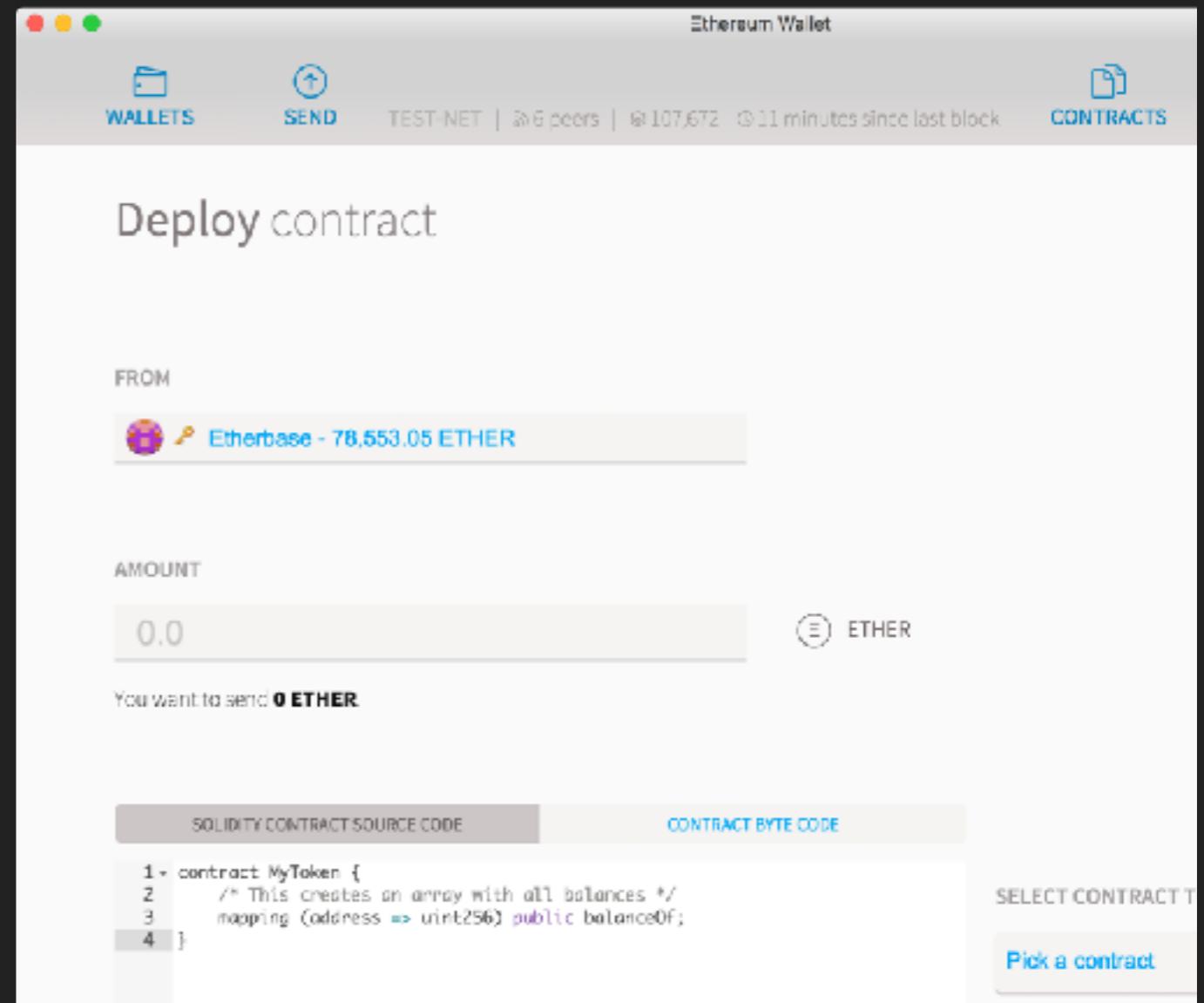
Main Account (ETHERBASE)
15,573,027.80 USD
0x5cc507A5ABb3ca63a4e37c26D61a0e87c0B0dFB4

+ ADD ACCOUNT

WALLET CONTRACTS

SMART CONTRACTS

- ▶ Expanded Bitcoin
- ▶ Store more than just currency
- ▶ Transactions -> mini programs
- ▶ Rudimentary stage
- ▶ Everybody can agree on : What happened and When
- ▶ Oracles needed



THE \$55M DAO HEIST

7/17/16:

I think TheDAO is getting drained right now

self.ethereum

Submitted 1 year ago by ledgerwatch



[–] 5chdn Flair 28 points 1 year ago

Just in case anyone wonders: **ETHEREUM IS NOT BROKEN**, it just a flaw in a smart contract which holds 250 million usd worth of ETH (a.k.a. The DAO).

[permalink](#) [embed](#) [parent](#)

10/6/17:



Ethereum Classic (ETC)

\$12.09 (1.06%)

Buy / Sell Insta

0.00277867 BTC (0.65%)

Website

Explorer

Announcement

Rank 11

Market Cap

\$1,162,979,261

267,330 BTC

Volume (24h)

\$28,528,500

6,558 BTC

Circulating Supply

96,207,811 ETC

MICRO INSURANCE



- ▶ Flight, Crop, Death, Illness, etc.

STOCKS

Delaware General Assembly

Enter Bill Number, Legislator, or Keyword 

BILLS & RESOLUTIONS DELAWARE LAWS COMMITTEES SENATE HOUSE OFFICES & SERVICES EVENTS & FACILITIES

[View All Legislation](#)
[View All Senate Legislation](#)
[View All House Legislation](#)

Senate Bill 69
149th General Assembly (Present)

Bill Progress

Current Status: Signed 7/21/17

What happens next? Becomes effective upon date of signature of the Governor or upon date specified

Bill Details

Introduced on: 5/5/17

Primary Sponsor: Townsend

Additional Sponsor(s): Sen. Delcollo, Hansen, Henry
Reps. Mitchell, Lynn, M. Smith

Co-Sponsor(s): Sen. Lavelle
Reps. Brady, J. Johnson, Paradee, Spiegelman

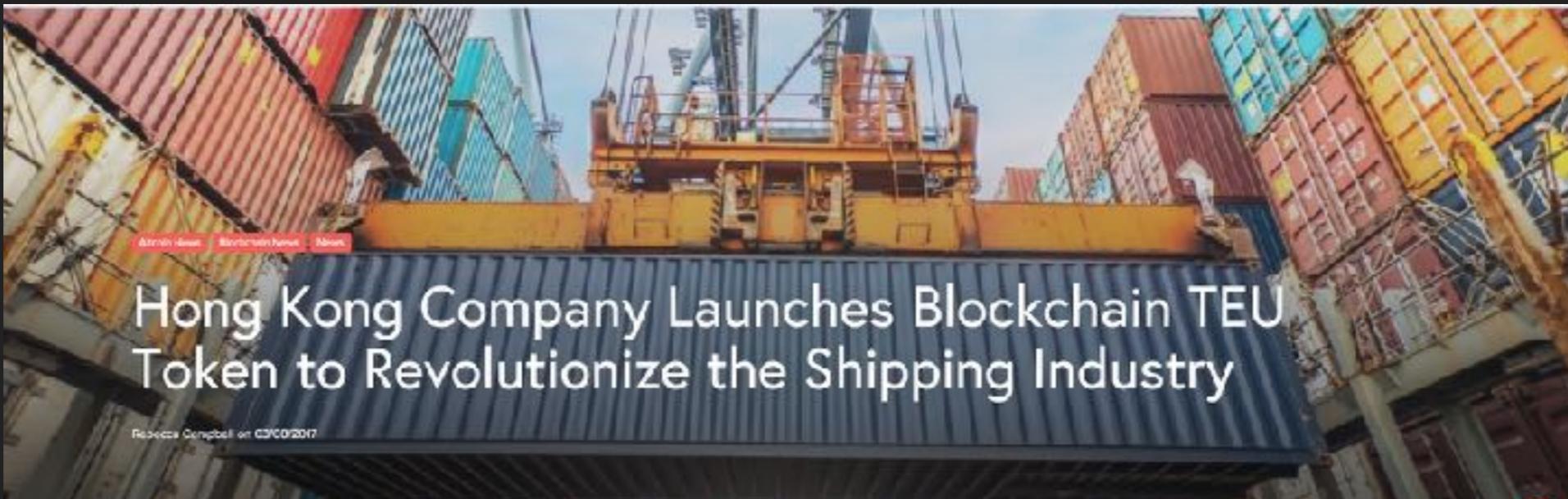
Long Title: AN ACT TO AMEND TITLE 8 OF THE DELAWARE CODE RELATING TO THE GENERAL CORPORATION LAW.

Original Synopsis: Section 1. Sections 1, 2, 5, 6, 7, 11 and 36 of this Act amend Sections 151(f), 202(a), 219(a), 219(c), 224, 232(c) and 364 of Title 8, respectively. Amendments to Sections 219, 224 and 232 and related provisions are intended to provide specific statutory authority for Delaware corporations to use networks of electronic databases (examples of which are described currently as "distributed ledgers" or a "blockchain") for the creation and maintenance of corporate records, including the corporation's stock ledger. Section 219(c), as amended, now includes a definition

▶ Also NV, AZ

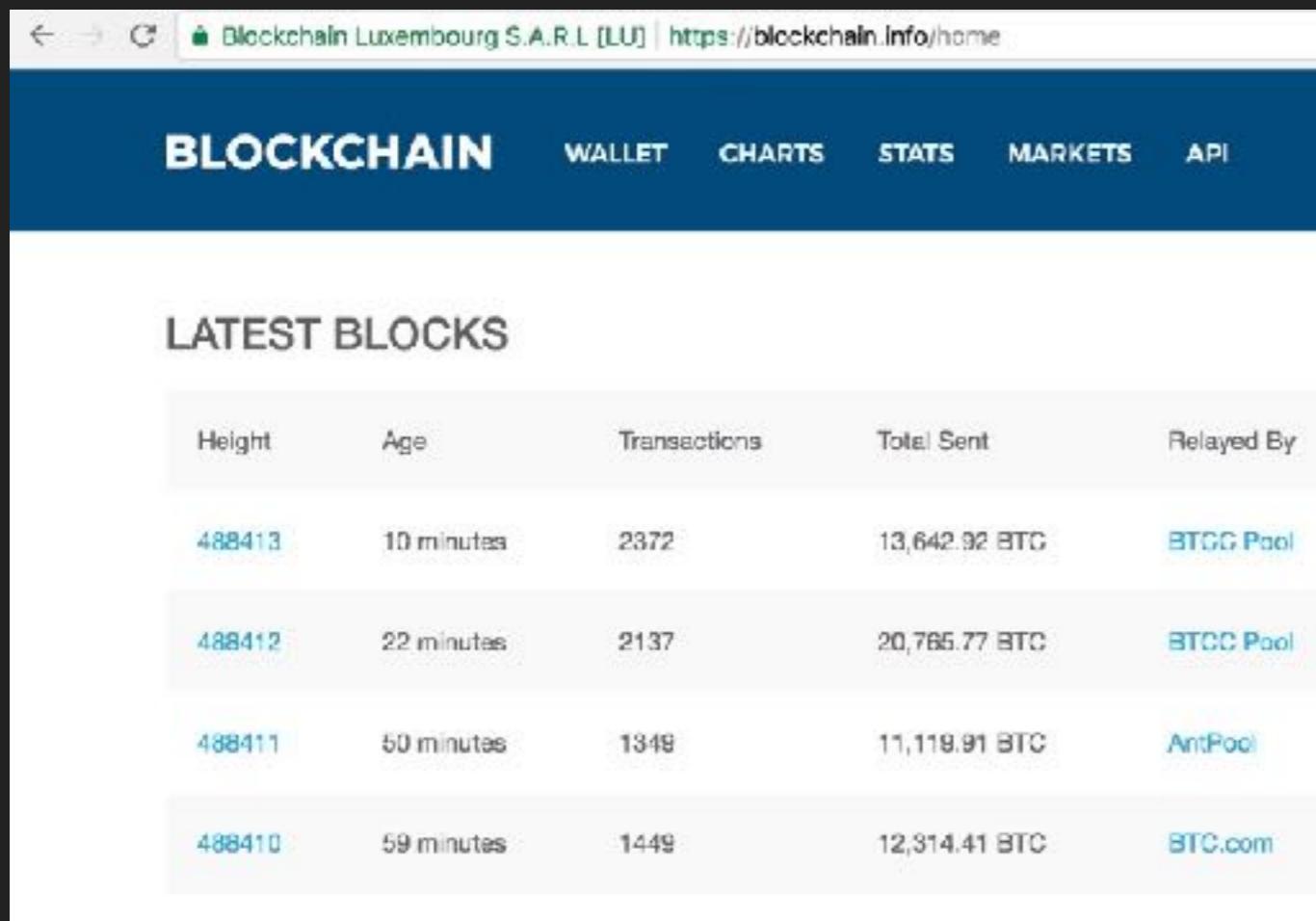
▶ T0

SUPPLY CHAIN



- ▶ Walmart-IBM
- ▶ SmartLog - IoT
- ▶ 300Cubits - TEU
- ▶ Maersk - POC

MINING



The screenshot shows the Blockchain.info homepage with a navigation bar at the top labeled 'BLOCKCHAIN', 'WALLET', 'CHARTS', 'STATS', 'MARKETS', and 'API'. Below the navigation bar, there is a section titled 'LATEST BLOCKS' which displays five recent blocks. Each block entry includes the height, age, number of transactions, total BTC sent, and the mining pool that relayed it.

Height	Age	Transactions	Total Sent	Relayed By
488413	10 minutes	2372	13,642.92 BTC	BTGG Pool
488412	22 minutes	2137	20,785.77 BTC	BTCC Pool
488411	50 minutes	1349	11,118.91 BTC	AntPool
488410	59 minutes	1449	12,314.41 BTC	BTC.com

- ▶ Process of adding transaction records to the blockchain
- ▶ Goal: tamper-resistance
- ▶ Intentionally resource-intensive
- ▶ Change the Nonce so the hash starts with a certain number of zeros
- ▶ Reward: 12.5 BTC

LIVE MINING

The screenshot shows a live mining interface with a toolbar at the top and a log of mining activity below. The toolbar includes buttons for Reveal, Now, Clear, Reload, Share, and Search. The log displays a series of mining events:

```
INFO [10-04|09:34:18] Commit new mining work
INFO [10-04|09:34:21] Successfully sealed new block
INFO [10-04|09:34:21] ⚡ block reached canonical chain
INFO [10-04|09:34:21] ↗ mined potential block
INFO [10-04|09:34:21] Commit new mining work
INFO [10-04|09:34:23] Updated mining threads
INFO [10-04|09:34:24] Successfully sealed new block
INFO [10-04|09:34:24] ⚡ block reached canonical chain
INFO [10-04|09:34:24] ↗ mined potential block
INFO [10-04|09:34:24] Commit new mining work
INFO [10-04|09:34:26] Successfully sealed new block
INFO [10-04|09:34:26] ⚡ block reached canonical chain
INFO [10-04|09:34:26] ↗ mined potential block
INFO [10-04|09:34:26] Commit new mining work
INFO [10-04|09:34:26] Successfully sealed new block
INFO [10-04|09:34:26] ⚡ block reached canonical chain
INFO [10-04|09:34:26] ↗ mined potential block
INFO [10-04|09:34:26] Commit new mining work
INFO [10-04|09:34:27] Successfully sealed new block
INFO [10-04|09:34:27] ⚡ block reached canonical chain
```

On the right side of the log, there is a column of mining details:

number	txs	uncles	elapsed
15293	0	0	176.973µs
15293			hash=d0b875..0e93b3
15288			hash=b4d262..377ea6
15293			hash=d0b875..0e93b3
15294	0	0	196.157µs
15294			threads=1
15294			hash=41c82d..987ec8
15289			hash=09b71d..2dcd74
15294			hash=41c82d..987ec8
15295	0	0	130.826µs
15295			hash=d05f4f..63be65
15290			hash=0657bf..3d95a4
15295			hash=d05f4f..63be65
15296	0	0	299.405µs
15296			hash=fbd5fd..0e5c19
15291			hash=6dfb41..af4267
15296			hash=fbd5fd..0e5c19
15297	0	0	209.432µs
15297			hash=757cb7..4e0cbe
15292			hash=fa4a42..019da9

MINING SECURITY

- ▶ Malware, botnets
- ▶ Harvard's Odyssey ('14), NSF ('14),
Federal Reserve ('17)
- ▶ 51% attack

BLOCK CHAIN PLATFORMS

- ▶ Hyperledger (Fabric, Sawtooth)
- ▶ IBM (Bluemix)
- ▶ Ripple (Banks)
- ▶ R3 (Corda)
- ▶ Quorum (JP Morgan)
- ▶ Microsoft's Coco (any blockchain)
- ▶ Microsoft's Azure (BaaS)

RAPID START UP - AZURE

The screenshot shows the Microsoft Azure portal interface for a deployment named "ethereum". The deployment status is "Succeeded" with a duration of "7 minutes 50 seconds". It was deployed to the "jsbc" resource group and is related to "Events". The template link is <https://gallery.azure.com/artifact/20161101/microsoft-ethereum-blockchain>. The deployment has three outputs: "ADMIN-SITE" with the value <http://jsbcv5mg7.eastus.cloudapp.azure.com>; "ETHEREUM-RPC-ENDPOINT" with the value <http://jsbcv5mg7.eastus.cloudapp.azure.com:8545>; and "SSH-TO-FIRST-TX-NODE" with the value `ssh -p 3000 gethadmin@jsbcv5mg7.eastus.cloudapp...`.

Deployment	Value
STATUS	Succeeded
DURATION	7 minutes 50 seconds
RESOURCE GROUP	jsbc
RELATED	Events
TEMPLATE LINK	https://gallery.azure.com/artifact/20161101/microsoft-ethereum-blockchain
Outputs	
ADMIN-SITE	http://jsbcv5mg7.eastus.cloudapp.azure.com
ETHEREUM-RPC-ENDPOINT	http://jsbcv5mg7.eastus.cloudapp.azure.com:8545
SSH-TO-FIRST-TX-NODE	<code>ssh -p 3000 gethadmin@jsbcv5mg7.eastus.cloudapp...</code>

QUESTIONS?

THANKYOU!